Interpol identifie près de 9000 serveurs infectieux en Asie

Ce pourrait être un gros coup prochainement porté à la cybercriminalité. Interpol a annoncé avoir identifié quelque 8□800 serveurs de Commande et Contrôle (CC) répartis sur huit pays d'Asie du Sud-Est. Ces machines à la solde de pirates peuvent être utilisées pour lancer des attaques massives par déni de service (DDoS), des campagnes de spam/phishing, servir de centre de téléchargement de malwares, propager des ransomwares, etc.

270 sites piratés

Plus précisément, ces serveurs ont été créés à partir de près de 270 sites web infectés par du code malveillant exploitant une vulnérabilité dans la conception des sites, indique l'organisation internationale de lutte contre la criminalité dans son communiqué. Des sites gouvernementaux, qui détiennent potentiellement des données personnelles de citoyens, font partie des victimes, ajoute l'institution dont l'enquête a été confiée à la division IGCI (Interpol Global Complex for Innovation) dédiée aux technologies informatiques.

A titre d'illustration, Interpol déclare avoir notamment identifié des opérateurs de phishing, dont un affiche des liens vers le Nigeria. Un autre, basé en Indonésie, vend des kits d'hameçonnage sur le Darknet et a même posté des modes d'emploi de ses outils sous formes de vidéos Youtube. L'enquête se poursuit sur les activités des serveurs CC, ajoute l'organisation policière.

23 rapports

Interpol souligne l'importance de la coopération internationale, ainsi que celle avec des entreprises privées, pour mener à bien ce type d'enquête. Les informations ont ainsi été remontées suite à des enquêtes effectuées localement en Indonésie, Malaisie, Birmanie, Philippines, Singapour, Thaïlande et Vietnam. La Chine a également contribué à l'effort en fournissant des renseignements. Et des experts d'entreprises privées (Trend Micro, Kaspersky Lab, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet et Palo Alto Networks) ont aidé Interpol à préparer les repérages. *« Le partage d'information a été la base du succès de cette opération »,* explique Noboru Nakatani, responsable de l'IGCI, qui y voit un facteur essentiel dans l'efficacité de la coopération à long terme et dans l'activité quotidienne de contre la cybercriminalité.

Un travail de longue haleine que Interpol se garde de détailler. D'autant que l'opération n'est pas terminée. Il reste à mettre fin à l'exploitation de ces quelque 9000 serveurs infectés toujours en service, le rôle de l'organisation anti-criminelle s'étant pour l'instant limité au travail d'enquête. Un travail qui est concrétisé par la rédaction de 23 rapports détaillant les activités illégales constatées et suggérant les actions à prendre en conséquence. Actions qui ressortent désormais de la seule volonté des autorités nationales des pays concernés.

Lire également :

Interpol s’entraîne à combattre le darknet
Les 3 propositions de la France pour enrayer la course aux armements cyber
FIC 2017 : les démocraties face à leurs fragilités numériques

crédit photo © Oleksiy Mark – shutterstock